

Forum:[Hack Forums](#)

Thread: [Can a RAT from 2000 bypass modern day AV?](#)

CyberStrike - December 13, 2017, 2:32 am

I thought this would be an interesting experiment. So to start with the venerable Netbus 1.6 a mighty contender from 2000. Tracking it down was more of a chore than anything else, but finally found it. I decided on going with an old RAT that no longer is in use in the wild, and should really have 100% detection although I discovered a very different real world when testing.

Tools:

msfvenom
sigthief
hyperion

So here I will be trying to use Netbus 1.6 as the base, and seeing how much can be quickly done to make it more passable. I also added a message box, to keep it as original as possible.

So this is the original PATCH.EXE

<https://www.virustotal.com/#/file/bf7aa8fafd5b719841211eaea5e8a2d44f4b24482a9c0ed093098a302fa151fd/detection>

SHA-256 bf7aa8fafd5b719841211eaea5e8a2d44f4b24482a9c0ed093098a302fa151fd
File name 1002-1031fc4869c5c1397f9ddf1773e46c030dc845e5
File size 461.5 KB
Last analysis 2016-02-15 17:06:41 UTC

57/67

How it isn't 67/67 I have no idea.

The idea here is using the "PATCH.exe" as the template in msfvenom, we will output to a "exe-only". Also using x86/shikata_ga_nai 2 iterations. I create a new file

sha256sum patch.exe
bf612b1aa77c8f2e4510565aabdb0e705d3f0b904cf66ed168590b4255a3c42f patch.exe
patch.exe : (37/67)

<https://www.virustotal.com/#/file/bf612b1aa77c8f2e4510565aabdb0e705d3f0b904cf66ed168590b4255a3c42f/detection>

```
ls -al patch.exe  
-rw-r--r-- 1 root root 472576 Dec 13 01:48 patch.exe
```

So now we are bypassing 20 more AV's including some like BitDefender/Comodo

Now I go ahead and scramble the PE a bit to make it appear as though it is still unencrypted and save as "patch1.exe"

sha256sum patch1.exe

58bf61b8934929e52da34db05da050fc3716e29280fb6118f14137daee2ee4af patch1.exe

patch1.exe : (41/67)

<https://www.virustotal.com/#/file/58bf61b8934929e52da34db05da050fc3716e29280fb6118f14137daee2ee4af/detection>

As to why the detections went up here I can only guess that is due to using Hyperion a runtime crypter. Too much encryption can also raise flags with AVs.

Now I grabbed procmon from microsoft. Why? Well I need it's signature

sha256sum Procmon.exe

978f95fc63699f1e769663e32bae596148742b3038f743a51af346ca4d2f56d0

Now onto ripping the signature of the file using sigtheif.

Ripping signature to file!

Output file: /root/Downloads/procmon/Procmon.exe_sig

Signature ripped.

FIN.

And we place the signature that we ripped on over to our netbus file.

Output file: /root/patch1.exe_signed

Signature appended.

FIN.

After placing the signature ripped from Procmon into our "patch1.exe" file

patch1.exe_signed: (37/67)

<https://www.virustotal.com/#/file/558fe4f23688446fe5a15eb62ced31a9a90e97e45b216a849a62d76fb4804657/detection>

So in conclusion, could more have been done? Could we get around every AV? Maybe but this does show that modern AV's still struggle with catching even 17 year old remote administration tools. Now could more have been done? Yes, certainly, but the point was to test if we can bypass more AV's than just the default. Funny thing is that more encryption didn't help too much. So looking at newer solutions for compromising currently at hand it is very feasible that one can bypass AV solutions, perhaps not all solutions, but to an initial compromise, it is possible.

Armada - December 13, 2017, 4:29 am

Netbus, pfft.

Bo2K FTW! lol

Interesting read however.

CyberStrike - December 13, 2017, 4:49 am

Originally I looked for BO2k btw tried cult of the dead cow they had 5 DL links all dead. But I would have done BO2K.

Armada - December 13, 2017, 4:51 am

(Dec 13, 2017 05:49 AM)sirru5h Wrote: [\[CITE\]](#) Originally I looked for BO2k btw tried cult of the dead cow they had 5 DL links all dead. But I would have done BO2K.

Pretty sure I got my OG copy saved on disk somewhere, lemme see if I can find it today, we can play around with it again. lol

That shit was fun a holy hell back in the day. lol

CyberStrike - December 13, 2017, 4:55 am

OH memories, I'll look around a bit as well I may have one of those old disk holder box things with partitions between the disks the new ones you know 1.44 if I still got it anywhere that's the spot.

AyyLmao0o - December 13, 2017, 7:56 am

Very interesting, thanks for sharing.

CyberStrike - December 13, 2017, 8:19 am

Excellent, glad it was a bit informative.

Armada - December 13, 2017, 9:02 am

My fucking drive went DOA on me :(

RIP 1999-2001 memories. lol

CyberStrike - December 13, 2017, 9:06 am

(Dec 13, 2017 10:02 AM)Armada Wrote: [\[CITE\]](#) My fucking drive went DOA on me :(

RIP 1999-2001 memories. lol

: / Moment of silence please Be strong

If it's an HD you maybe able to toss it into the freezer pull it out tomorrow maybe you get 2 hrs where you can dd it real quick. If it's a 1.44 / 5.25 it's prolly toasted.

Armada - December 13, 2017, 9:55 am

(Dec 13, 2017 10:06 AM)sirru5h Wrote: [\[CITE\]](#) : / Moment of silence please Be strong

If it's an HD you maybe able to toss it into the freezer pull it out tomorrow maybe you get 2 hrs where you can dd it real quick. If it's a 1.44 / 5.25 it's prolly toasted.

Disk analysis says corrupt sectors, which is not surprising this things like almost 20 years old as a drive. lol, trying to salvage what I can, we will see....

CyberStrike - December 13, 2017, 10:39 am

(Dec 13, 2017 10:55 AM)Armada Wrote: [\[CITE\]](#) Disk analysis says corrupt sectors, which is not surprising this things like almost 20 years old as a drive. lol, trying to salvage what I can, we will see....

Good luck, I remember after Katrina I got an HD that was just caked in shit and mud for one week I threw it in a bucket and kept changing out the water, then I threw it into the garage for another week, booted right up.

BTW I went back and touched the file that was before Hyperion and I padded the exe since hyperion got 41 detections while the file just before was at 37
here is what I got

<https://www.virustotal.com/#/file/ab15542e3258092cc4a30cd8cb24a0273ba6ff0783ae3ff0fad141b4e>

[a878dc1/detection](#)

(35/67)

```
sha256sum patchenc.exe_signed
```

```
4866510c7036009b1f45f875c22e3328b7ee6bc8c81f64ed6ef14680ef53c65b patchenc.exe_signed
```

File padding

```
truncate -s 15M patchenc.exe_signed
```

```
ls -al patchenc.exe_signed
```

```
-rw-r--r-- 1 root root 15728640 Dec 13 11:27 patchenc.exe_signed
```

```
file patchenc.exe_signed
```

```
patchenc.exe_signed: PE32 executable (GUI) Intel 80386, for MS Windows
```

(As a side note I bet that on VT they are wondering if netbus is making a resurgence)

Friedrich Nietzsche - December 13, 2017, 10:44 am

Scantime isn't the problem, runtime is.

With scantime you can use a "real" packer instead of binary obfuscators and yield a fully FUD output (because the data will be encrypted anyways).

CyberStrike - December 13, 2017, 10:53 am

That is true runtime for example if you have automigration on like say with meterpreter, AV's instantly catch it. I've been messing with application shims as well although that is really more of a post exploitation / persistence thing. If anyone wants to see if they can get it FUD give it a shot it's netbus 1.6 it's on packetstorm.

Edit: One thing is that I am not using anything special it's just with minimal effort make an old RAT passable. If anything it's more of a reflection on the AV manufacturers who have more than known about this piece of software for over 17 years now.

0x1010 - January 28, 2018, 12:18 am

Thanks for the post very interesting and a great read for once on here.

SIM-3386134 - January 28, 2018, 12:24 am

(Dec 13, 2017 11:44 AM)Friedrich Nietzsche Wrote: [\[CITE\]](#) Scantime isn't the problem, runtime is.

With scantime you can use a "real" packer instead of binary obfuscators and yield a fully FUD output (because the data will be encrypted anyways).

I concur.

Nice thread OP.

CyberStrike - January 28, 2018, 4:12 am

Well thanks I appreciate all the positive comments and I hope it helped maybe gives some ideas.

Vyxn - January 28, 2018, 7:38 am

(Jan 28, 2018 05:12 AM)sirru5h Wrote: [\[CITE\]](#) Well thanks I appreciate all the positive comments and I hope it helped maybe gives some ideas.

It was a nice thread. Hope you do more research about it.

CyberStrike - January 28, 2018, 9:59 am

I may, it was really just an experiment at the time to see how good are AV's at picking up old

malware, as was stated runtime would be a different game. Although I got an idea or two on dealing with that as well, and also another way that I can bypass just scans.

enmafia2 - January 28, 2018, 10:03 am

Very interesting idea, might give it a shot myself too.

Good job sirru5h

CyberStrike - January 28, 2018, 11:11 am

Just spent a bit of time in the hexeditor

<https://www.virustotal.com/#/file/9d5b7054100ca945a7640ea82ef51ed24154f83fe8804c71421b68768fee99b6/detection>

I suggest taking a look at "Taking Back Netcat" I would post a link but it is a PDF, and it is quite easy to find with a Google search.

Tools Used:

Ghex
virtualbox (windows 7 Enterprise VM)
ollydbg
NetCat 1.6 patch4
AVSignSeek
Calc
readpe

To determine where the signature(s) were I decided to break up the file into "sections" with no one file with the full payload as I would edit and see if it was detected.

AV's scanned by:

Kaspersky
Mcafee
Sophos

So the setup worked as the following first the complete payload is zipped with a password, thus denying AV access to the payload so the AV will only be able to scan the parts that are most likely to contain the signature(s)

Now full disclosure I got the idea not just from Taking Back Netcat but also AVSignSeek project on Github.

<https://github.com/hegusung/AVSignSeek>

First I inspected the file with readpe

Magic number:	0x10b (PE32)
Linker major version:	2
Linker minor version:	25
Size of .text section:	0x54800
Size of .data section:	0x1ea00

Size of .bss section: 0
Entrypoint: 0x55678
Address of .text section: 0x1000
Address of .data section: 0x56000

(Now I know where the important sections are going to be in the file.(Not full output))

I didn't use AVSignSeek the file although the trial and error manual method is lengthy the editing was done using ghex. So as per "Taking Back Netcat" I followed the steps I noticed that netbus had a few signatures. I had 7 different parts the from each file I would pretty much just replace it with 0x00 then I would scan the file, I found that there were multiple signatures, which at best would be impossible to make it "FUD". But it did give me an idea of where the signatures would be. (Note: AVSignSeek does not deal with multiple signitures)

As each section would be detected I would break up that file once again using 0x00 for various addresses pretty much one by one. (This is slow work here and had worked on it a bit last night) After finishing out all the testing I went back to the original file made a copy and edited in ghex the majority of areas that AV would detect the signature. At the end Netbus passed the AV solutions I was testing against, so I went ahead and uploaded to VT (Yes I know they will distribute but also who is using Netbus now a days? it's 2018). So as you can see from the results 15/64, that is 49 modren day AVs, that have been bypassed.

Now I have a few ideas on scantime bypass, but that is for another day. I wanted to add that there was no use of anything else no crypter, or automated obfuscation tools.

Baud - January 28, 2018, 11:50 am

Now this was a very interesting read. I couldn't help but notice how most of the AVs that still flag the latest executable as malicious detect it as NetBus instead of a generic threat, so there still are some signatures left that if changed could bring the detection rate even lower.

CyberStrike - January 28, 2018, 12:07 pm

Yeah I think that to bypass all those AV's it'd be a while and a ton of testing. One thing is that several AV companies just basically steal signatures from one another.. Kaspersky did this a while back they flagged a non-malicious file and many of the other AV companies followed suit. I'll try to find that article.

https://www.theregister.co.uk/2010/02/10/kaspersky_malware_detection_experiment/

[BLANK] - January 30, 2018, 8:22 am

Nice read! I wonder though would NetBus still be effective as a RAT? I suppose that could be a reason why some AV don't detect it if they don't believe it would be an issue even if it was allowed to execute. Also, many of those vendors were probably not around 17 years ago and may not have signatures much older then their inception.

Still, it sounds like a fun experiment. And you never know when you may run into that legacy system and a newer RAT would completely fail to execute on.

3azraiell - January 30, 2018, 9:13 am

let me now if you tested Bifrost

i used to use it on 2009 as my first rat hehehe

CyberStrike - January 30, 2018, 9:59 am

(Jan 30, 2018 09:22 AM)EasyGhost Wrote: [\[CITE\]](#) Nice read! I wonder though would NetBus still be effective as a RAT? I suppose that could be a reason why some AV don't detect it if they don't

believe it would be an issue even if it was allowed to execute. Also, many of those vendors were probably not around 17 years ago and may not have signatures much older than their inception.

Still, it sounds like a fun experiment. And you never know when you may run into that legacy system and a newer RAT would completely fail to execute on.

Thanks, it was interesting to actually do it manually I think if anything I learned a bit doing it that way than trying to just using AVSignSeek which wouldn't deal with multiple signatures, although that goes only so far without putting a whole lot of effort. You know I thought that maybe they would pay for previous signatures, it's like saying cyber warfare is the new thing so let's forget about having infantry.

A note on compatibility I used a 32bit Windows 7 it actually worked I didn't have to use compatibility mode. Gotta love how Windows just holds onto that backwards compatibility.

(Jan 30, 2018 10:13 AM)3azraiell Wrote: [\[CITE\]](#) let me now if you tested Bifrost i used to use it on 2009 as my first rat hehehe

I did a quick search on BitFrost and it seems that it may still be in use, so I wouldn't want to scan especially since it may screw over users of that product, that is the main reason I used something quite old.

TommyHilfiger - March 28, 2018, 5:34 am

did you try to assemble obscurely crafted payload in memory cave

CyberStrike - March 28, 2018, 9:39 am

Nope I didn't just basically used this file as a template and kept it working I didn't put any new anything into that file. I didn't even run too many iterations when encoding. I wanted pretty much to have it as "stock" as possible, only thing I did was just use msfvenom then objcopy for each section it's rather detailed in "Taking back Netcat"

TommyHilfiger - March 28, 2018, 11:59 am

yeah right i have read now whole thread
amazing lab work

05317832892 - March 30, 2018, 3:49 pm

Any RAT can be made scantime FUD.

The challenge would be run-time. You have to figure out how to disrupt memory signatures and patch out artifacts like statically named mutexes.

Bluffer - March 30, 2018, 3:52 pm

What surprised me most about this is that its antiviruses like Avast Mobile and Kingsoft that aren't detecting it. I've always thought Kingsoft was one of the best. Obviously not.

Great experiment OP.

05317832892 - March 31, 2018, 12:34 am

(Mar 30, 2018 03:52 PM)?luffer Wrote: [\[CITE\]](#) What surprised me most about this is that its antiviruses like Avast Mobile and Kingsoft that aren't detecting it. I've always thought Kingsoft was one of the best. Obviously not.

Great experiment OP.

Avast mobile won't be detecting PE malware lmao.

CyberStrike - April 1, 2018, 9:48 pm

(been a bit under the weather past few days) Runtime between obfuscating payloads, using a legit ssl certificate for communications to c2 and using code signing certs then perhaps using encryption for the memory addresses to prevent ease of carving out the payload from the RAM would go a long way to helping deal with AV.

<https://github.com/JLospinoso/gargoyle>

nwujks5103 - September 21, 2018, 12:07 am

Thanks for the post very interesting and a great read for once on here.

Business - September 21, 2018, 1:10 am

When testing against that many AVs, you're rarely going to find one that's detected by every single one because some of the companies no longer (or never did) update their definitions. That's why they slip through on your test.